REDACTED DOCUMENT

Docket # 18

Date Filed: 7/19/12

EL/GSG/2009R00080

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA : Hon. Jerome B. Simandle
:
v. : Criminal No. 09-626 (JBS)
:
VLADIMIR DRINKMAN, : 18 U.S.C. §§ 371, 1030, 1343, 1349, and 2
a/k/a :
a/k/a :
a/k/a :
:
ALEKSANDR KALININ, :
a/k/a :
a/k/a :
a/k/a :
a/k/a :
a/k/a :
a/k/a and :
:
MIKHAIL RYTIKOV, :
a/k/a :
a/k/a :
a/k/a :
a/k/a :
:

RECEIVED
JUL 1 9 2012
AT 8:30__________M
WILLIAM T. WALSH, CLERK

FILED
JUL 1 9 2012
AT 8:30__________M
WILLIAM T. WALSH
CLERK

SUPERSEDING INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges:

COUNT 1
(Conspiracy)
18 U.S.C. § 371
(All Defendants)

1. At various times relevant to this Superseding Indictment:

The Defendants

a. Defendant VLADIMIR DRINKMAN, a/k/a a/k/a a/k/a ("DRINKMAN") resided in or near St. Petersburg, Russia.

b. Defendant ALEKSANDR KALININ, a/k/a a/k/a a/k/a a/k/a a/k/a a/k/a ("KALININ") resided in or near St. Petersburg, Russia.

c. Defendant MIKHAIL RYTIKOV, a/k/a a/k/a a/k/a a/k/a ("RYTIKOV") resided in or near Ukraine.

Coconspirators

d. Albert Gonzalez, a/k/a a/k/a a/k/a ("Gonzalez"), a coconspirator who is not charged as a defendant herein, resided in or near Miami, Florida.

e. Damon Patrick Toey ("Toey"), a coconspirator who is not charged as a defendant herein, resided in or near Virginia Beach, Virginia and in or near Miami, Florida.

f. Co-Conspirator-1 ("CC #1"), a coconspirator who is not charged as a defendant herein, resided in or near Russia.

Methods of Hacking Utilized by Defendants

g. Structured Query Language ("SQL") was a computer programming language designed to retrieve and manage data in computer databases.

h. "SQL Injection Attacks" were methods of hacking into and gaining unauthorized access to computers connected to the Internet.

i. "SQL Injection Strings" were a series of instructions to computers used by hackers in furtherance of SQL Injection Attacks.

j. "Malware" was malicious computer software programmed to, among other things, gain unauthorized access to computers; to identify, store, and export information from hacked computers, including information such as user names and passwords ("Log-In

Credentials"), means of identification ("Personal Data"), and credit and debit card numbers and corresponding personal identification information of cardholders ("Card Data"); and to evade detection of intrusions by anti-virus programs and other security features running on those computers.

<u>The Corporate Victims of Computer Hacking</u>

k. NASDAQ was the largest United States electronic stock market, and the primary market for trading in the stocks of approximately 3,200 public companies. NASDAQ offered its customers access to on-line accounts over the Internet, and its computer network was located in, among other places, Middlesex County, New Jersey. Beginning in or about May 2007, NASDAQ was the victim of a SQL Injection Attack that resulted in the placement of malware on its network.

l. 7-Eleven, Inc. ("7-Eleven") was headquartered in Dallas, Texas, and was the corporate parent of a convenience store chain by the same name. 7-Eleven processed credit and debit card transactions through its computer networks. Beginning in or about August 2007, 7-Eleven was the victim of a SQL Injection Attack that resulted in malware being placed on its network and the theft of an undetermined number of credit and debit card numbers and corresponding Card Data .

m. JCPenney, Inc. ("JCP") was a major national retailer with its headquarters in Plano, Texas. JCP processed credit card payments for its retail stores through its computer network. Beginning on or about October 23, 2007, JCP was the victim of a SQL Injection Attack that resulted in the placement of malware on its network.

n. Hannaford Brothers Co. ("Hannaford") was a regional supermarket chain with stores located in Maine, New Hampshire, Vermont, Massachusetts, and New York that processed credit and debit card transactions through its computer network. In or about early November 2007, a related company of Hannaford was the victim of a SQL Injection Attack that resulted in the later placement of malware on Hannaford's network and the theft of approximately 4.2 million credit and debit card numbers and corresponding Card Data.

o. Heartland Payment Systems, Inc. ("Heartland"), which was located in or near Princeton, New Jersey and Plano, Texas, among other places, was one of the world's largest credit and debit card payment processing companies. Heartland processed millions of credit and debit transactions daily. Beginning on or about December 26, 2007, Heartland was the victim of a SQL Injection Attack on its corporate computer network that resulted in malware being placed on its payment processing system and the theft of more than approximately 130 million credit and debit card numbers and corresponding Card Data.

p. Wet Seal, Inc. ("Wet Seal") was a major national retailer with its headquarters in Foothill Ranch, California. Wet Seal processed credit and debit card payments for its retail stores through its computer network. In or about January 2008, Wet Seal was the victim of a SQL Injection Attack that resulted in the placement of malware on its network.

q. Dexia Bank Belgium ("Dexia") was a consumer bank located in Belgium. Between in or about February 2008 and in or about February 2009, Dexia was the victim of SQL Injection Attacks that resulted in the placement of malware on its network and the theft of Card Data that resulted in approximately $1.7 million in loss.

r. Jet Blue Airways ("Jet Blue") was an airline serving approximately 64 cities in the United States, Carribean, Central and South America, with its headquarters in Long Island City, New York. Between in or about January 2008 and in or about February 2011, Jet Blue suffered an unauthorized intrusion resulting in the placement of malware on portions of its computer network that stored Personal Data of its employees.

s. Dow Jones, Inc. ("Dow Jones") published news, business, and financial information worldwide in newspapers, on television and radio, over news wires, and on the Internet. Dow Jones' computer infrastructure was based largely in New Jersey, as well as in Minnesota, New York and elsewhere. In or before 2009, Dow Jones was the victim of unauthorized access to its computer network resulting in the placement of malware on its network and the theft of approximately 10,000 sets of Log-In Credentials.

t. Euronet was a global provider of electronic payment and transaction processing solutions for financial institutions, retailers, service providers and individual consumers, with its headquarters in Leawood, Kansas. Between in or about July 2010 and in or about October 2011, Euronet was the victim of SQL Injection Attacks that resulted in the placement of malware on its network and resulted in the theft of approximately 2 million credit and debit card numbers and corresponding Card Data.

u. Global Payment Systems ("Global Payment") was one of the world's largest electronic transaction processing companies, with its headquarters in Atlanta, Georgia. Between in or about January 2011 and in or about March 2012, Global Payment was the victim of SQL Injection Attacks on its computer network that resulted in malware being placed on its payment processing system and the theft of more than 950,000 credit and debit card numbers and corresponding Card Data.

v. NASDAQ, 7-Eleven, JCP, Hannaford, Heartland, Wet Seal, Dexia, Jet Blue, Dow Jones, Euronet, and Global Payment are collectively referred to herein as the "Corporate Victims."

THE CONSPIRACY

2. Between in or about August 2005 and in or about July 2012, in Mercer, and Middlesex Counties, in the District of New Jersey, and elsewhere, defendants

VLADIMIR DRINKMAN,
a/k/a
a/k/a
a/k/a

ALEKSANDR KALININ,
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a and

MIKHAIL RYTIKOV,
a/k/a
a/k/a
a/k/a
a/k/a

did knowingly and intentionally conspire and agree with each other, Gonzalez, Toey, CC #1, and others to commit offenses against the United States, namely:

a. by means of interstate communications, intentionally accessing computers in interstate commerce without authorization, and exceeding authorized access, and thereby obtaining information from those computers, namely Log-In Credentials, Personal Data, and Card Data, for the purpose of commercial advantage and private financial gain, contrary to Title 18, United States Code, Sections 1030(a)(2)(c) and (c)(2)(B)(I); and

b. knowingly and with intent to defraud accessing computers in interstate commerce without authorization and exceeding authorized access to such computers, and by means of such conduct furthering the intended fraud and obtaining anything of value, namely Log-In Credentials, Personal Data, and Card Data, contrary to Title 18, United States Code, Section 1030(a)(4).

OBJECT OF THE CONSPIRACY

3. It was the object of the conspiracy for DRINKMAN, KALININ, RYTIKOV, Gonzalez, Toey, CC #1, and others to hack into the Corporate Victims' computer networks in order to steal and then sell Log-In Credentials, Personal Data, and Card Data, or to otherwise profit from their unauthorized access.

MANNER AND MEANS OF THE CONSPIRACY

4. The manner and means by which DRINKMAN, KALININ, RYTIKOV, Gonzalez, Toey, CC #1, and others, sought to accomplish the conspiracy included, among other things, the following:

Scouting Potential Victims

a. It was part of the conspiracy that Gonzalez and Toey would identify potential corporate victims, by, among other methods, reviewing a list of Fortune 500 companies.

b. It was further part of the conspiracy that Gonzalez and Toey would travel to retail stores of potential corporate victims, both to identify the payment processing systems that the would-be victims used at their point of sale terminals (e.g., "checkout" computers) and to understand the potential vulnerabilities of those systems.

c. It was further part of the conspiracy that KALININ, Gonzalez, and Toey would visit potential corporate victims' websites to identify potential vulnerabilities of those systems.

Launching the Attacks – The Hacking Platforms

d. It was further part of the conspiracy that KALININ, Gonzalez, and others would lease, control, and use Internet-connected computers in New Jersey ("the Net Access Server"), Pennsylvania ("the BurstNet Server"), California ("the ESTHOST Server"), Illinois ("the Gigenet Server"), Latvia ("the Latvian Server"), the Netherlands ("the Leaseweb Server"), Ukraine, the Bahamas, Panama, and elsewhere (collectively, "the Hacking Platforms") to (1) store malware; (2) stage attacks on the Corporate Victims' networks; and (3) receive stolen Log-In Credentials, Personal Data, and Card Data from these networks.

e. It was further part of the conspiracy that RYTIKOV would lease some of the Hacking Platforms to KALININ for use in attacking the Corporate Victims' networks.

f. It was further part of the conspiracy that DRINKMAN, KALININ, Gonzalez, and Toey would provide each other and others with SQL Injection Strings and malware that could be used to gain unauthorized access to the Corporate Victims' networks and to locate, store, and transmit Log-In Credentials, Personal Data, and Card Data from those networks.

g. It was further part of the conspiracy that DRINKMAN, KALININ, Gonzalez, and Toey would hack into the Corporate Victims' networks using various techniques, including, among others, SQL Injection Attacks, to steal, among other things, Log-In Credentials, Personal Data, and Card Data.

Executing the Attacks - The Malware

h. It was further part of the conspiracy that once they hacked into the computer networks, DRINKMAN, KALININ, and Gonzalez would place unique malware on the Corporate Victims' networks that would enable them to access these networks at a later date ("Back Doors").

i. It was further part of the conspiracy that once they hacked into the Corporate Victims' networks, DRINKMAN, KALININ, and Gonzalez would conduct network reconnaissance for the purpose of finding and stealing Log-In Credentials, Personal Data, and Card Data within the Corporate Victims' networks.

j. It was further part of the conspiracy that once DRINKMAN, KALININ, and Gonzalez hacked into the Corporate Victims' networks, they would install "sniffer" programs that would capture credit and debit card numbers, corresponding Card Data, and other information on a real-time basis as the information moved through the Corporate Victims' credit and debit card processing networks, and then periodically transmit that information to the coconspirators.

k. It was further part of the conspiracy that DRINKMAN, KALININ, Gonzalez, and Toey would communicate via instant messaging services while the unauthorized access by them was taking place in order to advise each other as to how to navigate the Corporate Victims' networks and how to locate Log-In Credentials, Personal Data, and Card Data.

l. It was further part of the conspiracy that DRINKMAN, KALININ, and Gonzalez would use unique malware to transmit the Log-In Credentials, Personal Data, and Card Data to a Hacking Platform.

Concealing the Attacks

m. It was further part of the conspiracy that DRINKMAN, KALININ, Gonzalez, and Toey would conceal their efforts to hack into the Corporate Victims' networks by, among other things, leasing the Hacking Platforms under false names.

n. It was further part of the conspiracy that RYTIKOV offered "bullet-proof hosting" services to his coconspirators (i.e., leasing servers from which law enforcement supposedly could not gain access or obtain information). "Bullet-proof hosting" services included frequently changing the locations of Hacking Platforms, erasing the contents of Hacking Platforms on short notice, accepting false credentials to register and lease Hacking Platforms, and discouraging Internet Service Providers from deactivating Hacking Platforms suspected of illegal activity.

o. It was further part of the conspiracy that DRINKMAN, KALININ, Gonzalez, Toey, and others also concealed their efforts by communicating over the Internet using more than one messaging screen name, storing data related to their attacks on multiple Hacking Platforms, disabling programs that logged inbound and outbound traffic over the Hacking Platforms, and disguising, through the use of "proxies," the Internet Protocol addresses from which their attacks originated.

p. It was further part of the conspiracy that DRINKMAN, KALININ, Gonzalez, and Toey would conceal their efforts to hack into the Corporate Victims' networks by, among other things, programming malware to be placed on the Corporate Victims' computer networks to evade detection by anti-virus software.

Profiting from the Attacks

q. It was further part of the conspiracy that DRINKMAN, KALININ, Gonzalez, and Toey provided "CC #1" and others with the Log-In Credentials, Personal Data, and Card Data to sell through various on-line forums and other means.

OVERT ACTS

5. In furtherance of the conspiracy, and to effect its unlawful object, the coconspirators committed and caused to be committed the following criminal acts, among others, in the District of New Jersey and elsewhere:

NASDAQ and Jet Blue

a. On or about May 19, 2007, KALININ identified a security vulnerability at a NASDAQ web page that enabled NASDAQ's customers to obtain on-line password reminders ("the Remind Me Site").

b. On or before May 24, 2007, KALININ used a SQL Injection Attack to obtain encrypted Log-In Credentials from NASDAQ's Remind Me Site and sent it via instant message to Gonzalez.

c. On or about May 24, 2007, KALININ sent Gonzalez a SQL Injection String that Gonzalez could use to access NASDAQ's computer network without authorization.

d. On or about August 12, 2007, after KALININ accessed NASDAQ's computer network, KALININ sent Gonzalez an instant message stating that the network was about "30 SQL servers, and we can run whatever on them, already cracked admin PWS but the network not viewable yet." KALININ further commented that "those dbs are hell big and I think most of info is trading histories."

e. On or about January 9, 2008, in response to an offer from Gonzalez to help attack NASDAQ, KALININ told Gonzalez via instant message that "NASDAQ is owned."

f. On or before January 9, 2008, KALININ obtained administrative access to NASDAQ's computer network, and noted to Gonzalez via instant message that he had had that access for a long time.

g. On or about March 18, 2008, KALININ wrote to Gonzalez via instant message that DRINKMAN had lost "back door" access to NASDAQ, that KALININ had reacquired it, and that KALININ would not lose it again.

h. Between on or about August 28, 2008 and in or about March 2009, KALININ rented a Hacking Platform in the Bahamas ("the Bahamas Server") from RYTIKOV.

i. On or about November 26, 2008, KALININ caused the insertion of an unauthorized file named "hcx.txt" on the NASDAQ network. "hcx.txt" was pre-programmed to assist in communications with the Bahamas Server that KALININ rented from RYTIKOV.

j. On or about December 10, 2008, KALININ caused the insertion of hcx.txt on the Jet Blue network. "hcx.txt" was pre-programed to assist in communications with the Bahamas Server that KALININ rented from RYTIKOV.

k. In or about October 2009, a coconspirator caused a NASDAQ computer to attempt to communicate with the Bahamas Server that KALININ rented from RYTIKOV.

Heartland and JCP

l. On or about November 6, 2007, Gonzalez transferred a computer file named "sqlz.txt" that contained information stolen from JCP's computer network to a Hacking Platform in Ukraine ("the Ukraine Server").

m. On or about November 6, 2007, Gonzalez transferred a computer file to the Ukraine Server named "injector.exe" that matched malware placed on both Heartland and JCP's servers during the hacks of those companies.

n. On or about December 26, 2007, DRINKMAN and KALININ accessed Heartland's computer network by means of a SQL Injection Attack from the Leaseweb Server and using the ESTHOST Server.

o. Between in or about February 2008 and in or about March 2008, CC #1 sent "V.H." instant messages providing credit card and debit card numbers obtained by DRINKMAN and KALININ from the Heartland hack.

Wet Seal

p. In or about January 2008, over an internet messaging service, Gonzalez sent Toey a SQL Injection String that was used to penetrate Wet Seal's computer network (the "Wet Seal SQL String"). The Wet Seal SQL String was programmed to direct data to Hacking Platforms, including the ESTHOST Server and the Ukraine Server.

q. On or about April 22, 2008, Gonzalez modified a file on the Ukraine Server that contained computer log data stolen from Wet Seal's computer network.

r. Between in or after March 2007 and in or about May 2008, Gonzalez participated in a discussion over an internet messaging service in which one of the participants stated "core still hasn't downloaded that Wet Seal sh-t."

Hannaford

s. Between in or after March 2007 and in or about May 2008, Gonzalez participated in a discussion over an internet messaging service in which one of the participants stated "planning my second phase against Hannaford."

t. Between in or after December 2007 and in or about May 2008, Toey participated in a discussion over an internet messaging service in which one of the participants stated "that's how hacked Hannaford."

Dexia

u. Between in or about May 2008 and in or about August 2008, KALININ leased a Hacking Platform from RYTIKOV located in Panama ("the Panama Server").

v. Between in or about February 2008 and in or about August 2008, a coconspirator caused the insertion of a file named "L.exe" on Dexia's computer network. "L.exe," which allowed outside users to run programs on Dexia's network, was the same file used in the attacks on Heartland, NASDAQ, and JCP. Gonzalez also hosted the same file on the Ukraine Server.

w. On or about August 4, 2008, during the time that KALININ leased the Panama Server from RYTIKOV, KALININ caused Dexia Bank's network to establish a file transfer connection with the Panama Server.

x. On or about August 27 and August 28, 2008, KALININ instructed RYTIKOV via instant message to reinstall the operating system on the Panama Server, effectively erasing it, and to give this server to a different customer.

Dow Jones and the Odessa Server

y. On or about August 8, 2008, KALININ asked RYTIKOV via instant message to custom-build him a Hacking Platform.

z. Between on or about August 8, 2008 and on or about August 11, 2008, RYTIKOV built a Hacking Platform for KALININ that was located in Odessa, Ukraine ("the Odessa Server").

aa. On or about August 11, 2008, RYTIKOV gave access to the Odessa Server to KALININ and assigned it to a particular Internet Protocol address.

bb. Later that day, KALININ complained to RYTIKOV that the network speed to the Odessa Server was not fast enough for KALININ because KALININ needed to be able to download approximately 32 gigabytes of information at one time.

cc. On or about August 18, 2008, KALININ used the Odessa Server to store "rainbow tables," which were lists of possible passwords made for use with password-cracking software. The lists of possible passwords in rainbow tables were approximately 34 gigabytes in size.

dd. On or about December 13, 2008, in connection with providing "bullet-proof hosting" services, RYTIKOV's data center assigned the Odessa Server a new Internet Protocol address and advised KALININ via instant message the new Internet Protocol address for the Odessa Server.

ee. In or about February 2009, in connection with providing "bullet-proof hosting" services, RYTIKOV assigned the Odessa Server a new Internet Protocol address and advised KALININ via instant message of that new Internet Protocol address for the Odessa Server.

ff. On or about May 18, 2009, KALININ attempted to connect to the Odessa Server and told RYTIKOV via instant message that he was having trouble.

gg. Between in or about August 2008 and on or about June 24, 2009, KALININ used the Odessa Server to store and later delete approximately 30,000 sets of Log-In Credentials (mainly user names and encrypted passwords) belonging to Dow Jones employees and Dow Jones user accounts.

hh. Between on or about August 28, 2008 and on or about June 24, 2009, KALININ used the Odessa Server to open a file transfer connection with the Bahamas Server used in the attack on NASDAQ and Jet Blue.

Euronet

ii. Between in or about July 2010 and in or about December 2011, a coconspirator caused the insertion of a file named "medll.exe" on Euronet's computer network, which allowed outside users to run programs on Euronet's network from the German Leaseweb and Hetzner Online Servers. "medll.exe" used the same unique encryption key as the malware used in the Dow Jones and JCP intrusions described above, among others.

jj. Between in or about February 2010 and in or about April 2011, KALININ accessed the German Leaseweb and Hetzner Online Servers on multiple occasions, and on a number of occasions downloaded executable files from the German Leaseweb or Hetzner Online Servers, including malware.

Global Payment Systems

kk. In or about January 2011, a coconspirator caused the insertion of a file named "medll.exe" on Global Payment's computer network, which allowed outside users to run programs on Euronet's network from the German Leaseweb and Hetzner Online Servers. "medll.exe" used the same unique encryption key as the malware used in the Dow Jones, JCP, and Euronet intrusions described above, among others.

ll. In or about 2011, the German Leaseweb or Hetzner Online Servers were used to access Internet Protocol addresses associated with Global Payments.

All in violation of Title 18, United States Code, Section 371.

COUNT 2
(Conspiracy to Commit Wire Fraud)
18 U.S.C. § 1349

1. The allegations contained in paragraphs 1 and 3 of Count 1 of the Superseding Indictment are realleged and incorporated as if set forth herein.

2. Between in or about October 2006 and in or about July 2012, in Mercer and Middlesex Counties, in the District of New Jersey, and elsewhere, defendants

VLADIMIR DRINKMAN,
a/k/a
a/k/a
a/k/a

ALEKSANDR KALININ,
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a and

MIKHAIL RYTIKOV,
a/k/a
a/k/a
a/k/a
a/k/a

did knowingly and intentionally conspire and agree with each other, Gonzalez, Toey, CC #1, and others to devise a scheme and artifice to defraud the Corporate Victims, their customers, and the financial institutions that issued credit and debit cards to those customers, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing the scheme and artifice to defraud, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce,

COUNT 2
(Conspiracy to Commit Wire Fraud)
18 U.S.C. § 1349

1. The allegations contained in paragraphs 1 and 3 of Count 1 of the Superseding Indictment are realleged and incorporated as if set forth herein.

2. Between in or about October 2006 and in or about July 2012, in Mercer and Middlesex Counties, in the District of New Jersey, and elsewhere, defendants

VLADIMIR DRINKMAN,
a/k/a
a/k/a
a/k/a

ALEKSANDR KALININ,
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a and

MIKHAIL RYTIKOV,
a/k/a
a/k/a
a/k/a
a/k/a

did knowingly and intentionally conspire and agree with each other, Gonzalez, Toey, CC #1, and others to devise a scheme and artifice to defraud the Corporate Victims, their customers, and the financial institutions that issued credit and debit cards to those customers, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing the scheme and artifice to defraud, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

OBJECT OF THE CONSPIRACY

3. It was the object of the conspiracy for DRINKMAN, KALININ, Gonzalez, Toey, CC #1, and others to profit from the sale and fraudulent use of credit and debit card numbers and corresponding Card Data stolen from the Corporate Victims' computer networks.

MANNER AND MEANS OF THE CONSPIRACY

4. It was part of the conspiracy that once the coconspirators had stolen credit and debit card numbers and corresponding Card Data (the "Stolen Data") from the Corporate Victims' computer networks, DRINKMAN, KALININ, Gonzalez, Toey, CC #1, and others would cause the Stolen Data to be broken down into batches suitable for wholesale distribution over the Internet.

5. It was further part of the conspiracy that DRINKMAN, KALININ, Gonzalez, Toey, CC #1, and others would sell the Stolen Data using wire communications in interstate and foreign commerce and cause it to be available for resale.

6. It was further part of the conspiracy that those who purchased batches of the Stolen Data would further distribute the Stolen Data throughout the United States and elsewhere using wire communications in interstate and foreign commerce, where it would be used to make unauthorized purchases at retail locations, to make unauthorized withdrawals from banks and financial institutions, and to further identity theft schemes.

All in violation of Title 18, United States Code, Section 1349.

COUNTS 3-8
(Unauthorized Computer Access)
18 U.S.C. § 1030

1. The allegations contained in paragraphs 1, 4, and 5 of Count 1 of the Superseding Indictment are realleged and incorporated as if set forth herein.

2. On or about the dates set forth below, in Mercer and Middlesex Counties, in the District of New Jersey, and elsewhere, defendants

VLADIMIR DRINKMAN,
a/k/a
a/k/a
a/k/a

ALEKSANDR KALININ,
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a and

MIKHAIL RYTIKOV,
a/k/a
a/k/a
a/k/a
a/k/a

by means of interstate communications, did intentionally access computers without authorization, and exceeded authorized access to computers, namely the computer systems used in and affecting interstate and foreign commerce and communication owned by the Corporate Victims identified below, and thereby obtained information from those computers, namely Log-In Credentials, Personal Data, and Card Data, for the purpose of commercial advantage and private financial gain:

Count	Approximate Date	Corporate Victim
3	August 2007	7-Eleven
4	October 23, 2007	JC Penney
5	December 26, 2007	Heartland
6	January 2008	Wet Seal
7	January 2008	Jet Blue
8	2009	Dow Jones

In violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i).

COUNTS 9-11
(Wire Fraud)
18 U.S.C. § 1343

1. The allegations contained in paragraphs 1, 4, and 5 of Count 1 of the Superseding Indictment are realleged and incorporated as if set forth herein.

2. On or about the dates set forth below, in Mercer and Middlesex Counties, in the District of New Jersey, and elsewhere, defendants

VLADIMIR DRINKMAN,
a/k/a
a/k/a
a/k/a

ALEKSANDR KALININ,
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a and

MIKHAIL RYTIKOV,
a/k/a
a/k/a
a/k/a
a/k/a

did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud and to obtain money and property from the Corporate Victims identified below by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme or artifice, did knowingly transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, namely, Log-In Credentials and Card Data.

Count	Approximate Date	Corporate Victim
9	August 2007	7-Eleven
10	December 26, 2007	Heartland
11	2009	Dow Jones

In violation of Title 18, United States Code, Sections 1343 and Section 2.

A TRUE BILL

FOREPERSON

Paul J. Fishman

PAUL J. FISHMAN
United States Attorney

CASE NUMBER: 09-626

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

VLADIMIR DRINKMAN,
a/k/a
a/k/a
a/k/a

ALEKSANDR KALININ,
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a and

MIKHAIL RYTIKOV,
a/k/a
a/k/a
a/k/a
a/k/a

INDICTMENT FOR

18 U.S.C. §§ 371, 1030, 1343, 1349 and 2

A True Bill,

Foreperson

PAUL J. FISHMAN
U.S. ATTORNEY NEWARK, NEW JERSEY

EREZ LIEBERMANN / GURBIR GREWAL
ASSISTANT U.S. ATTORNEYS
(973) 645-2874

USAO#2009R00080